



MULTI-STATE
Information Sharing
& Analysis Center™

MS-ISAC THREAT BRIEF

ERIN DAYTON

WV CYBER SECURITY
CONFERENCE

OCTOBER 25, 2016

MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER



The U.S. Department of Homeland Security has designated the MS-ISAC as its key cybersecurity resource for cyber threat prevention, protection, response and recovery for all U.S. State, Local, Tribal and Territorial (SLTT) governments.

WHO WE SERVE

MS-ISAC Members include:

- All 56 US States and Territories
- All 78 federally recognized fusion centers
- More than 1,000 local governments and tribal nations

State, Local, Tribal, and Territorial

Cities, counties, towns, airports, public education, police departments, ports, transit associations, and more

HOW DO YOU KNOW YOU ARE A TARGET?

Knock, knock...



WHY GOVERNMENT?



Criminals look for data.....
And governments have a lot of it!

AFFECTED ENTITIES



Vulnerabilities

Content Management
Systems

Plug In's

Server

Web Programming
Language

Phishing

- ✓ Well Written
- ✓ Appear Credible
- ✓ Enticing or Shocking Subject
- ✓ Apparent Trusted Source



CYBER THREAT ACTORS



Nation-states



Terrorists



Cyber Criminals



Hactivists



Insiders

NATION STATE ACTORS/APT



Political
Leverage

Competitive
Insight

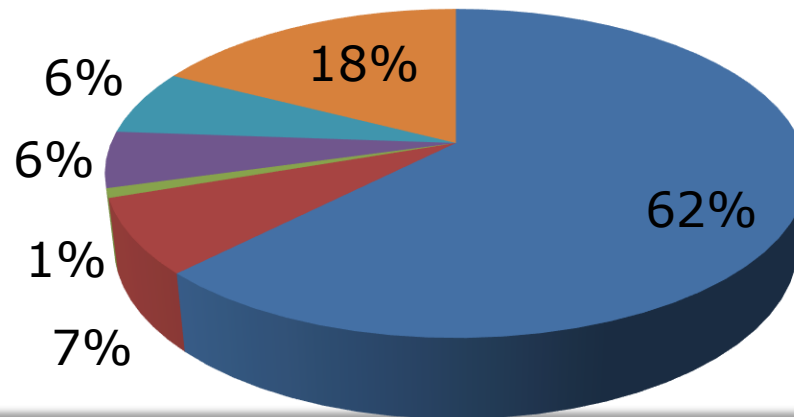
Intellectual
Capital

Cyber
Warfare

APRIL – MAY 2016 NATION-STATE CAMPAIGN

- 1 Campaign
- Targets predominantly ran Follett's Destiny software (K-12 schools)
- Total entities notified: 103

Impacted Entities



NATION-STATE SPEAR PHISHING

From: [REDACTED] [mailto:[REDACTED]@yahoo.com]
Sent: Thursday, June 20, 2012 7:53 AM
To: [REDACTED]
Subject: Homeland Security Assessment of [REDACTED]

Dear,
Please find attached and give some advice.
[http://www.devillas.com/report/Homeland_Security_Assessment_Of_\[REDACTED\].zip](http://www.devillas.com/report/Homeland_Security_Assessment_Of_[REDACTED].zip)
Regards,

Agency Director

Agency Deputy Director

Work related

Expected business need

Expected topic

From: Rebecca Jr. [mailto:rebecca.smith363@yahoo.com]
Sent: Thursday, June 20, 2013 6:20 AM
To: [REDACTED]
Subject: my new contact info

Unknown person

Government employee

Expected business need

Hey [REDACTED], this is Rebecca, and this is my new contact info. Besides, I find an old picture of our gathering last time. I now upload it on the website www.photogellrey.com/photo/group/dsc10006.asp?id=30041. Check it, see if you can recognize each one!

Implied relationship

UKRAINE'S CRITICAL INFRASTRUCTURE



Boryspil International Airport – Kiev, Ukraine

Power Grid Shut Down

80,000 customers lost power for 6 hours

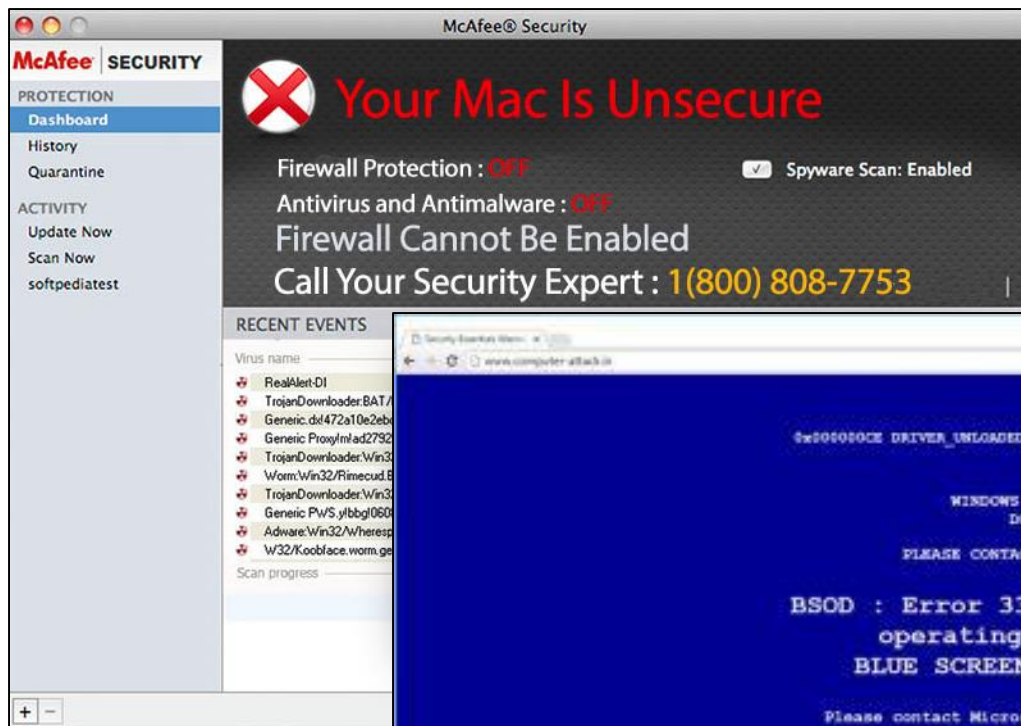
BlackEnergy Malware

IP Attributed to Russia

CYBER CRIMINALS



TECH SUPPORT CALL SCAM



BUSINESS EMAIL COMPROMISE

- From the CEO or Senior Executive
- To someone in the finance department
- Sense of urgency
- Abrupt text normal to an email from a phone

Date:

FROM: CEO

TO: Finance Department

SUBJECT: Question

Are you available? Wire transfer needs to go out. Also what is the balance of General Funding Account? Let me know when you are ready. Reply as soon as possible.

Sent from my iPhone



Hollywood Presbyterian Hospital

"The quickest and most efficient way to restore our system and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this."

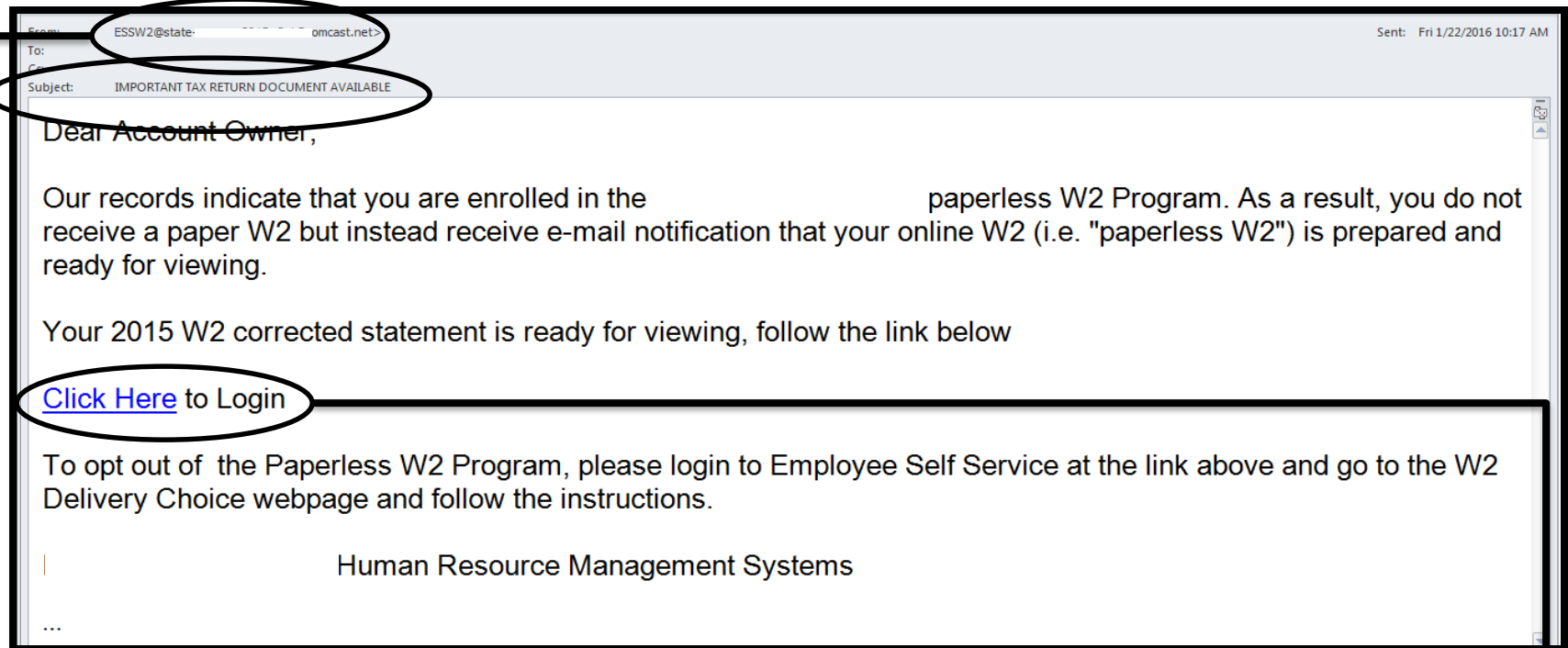
CASE STUDY

W-2 Phishing Campaign Targets States in Early-2016



MULTI-STATE
Information Sharing
& Analysis Center™

CREDENTIAL HARVESTING PHISHING EMAILS



**Spoofed email that appears as
ESSW2@[targeted domain]**

**Subject: IMPORTANT TAX RETURN
DOCUMENT AVAILABLE**

**Credential
Harvesting
Website**

MS-ISAC INVESTIGATION

- Opportunistic compromise of webpages running out-of-date versions of PHP
- Created mirrors of SLTT human resource web pages
 - These mirrored webpages URIs ended with "esslogin.htm"
- If a user follows the link in the phishing email, the user is directed to the compromised webpage and is prompted to log in
- Analysis of HTTP POST traffic indicates credentials entered (valid or not) are sent via Perl script to a hxxp://formbuddy.com account
- After the credentials have been submitted, the user is redirected to the legitimate targeted state website

HACKTIVISTS



YOU HAVE BEEN
HACKED !



DDoS
Attacks

Social,
Political &
Ideological
Agenda

Doxing

System
Compromise

Opportunistic

Targeted

Web
Defacements



MULTI-STATE
Information Sharing
& Analysis Center™

PERSONALITIES



Home user/ Student:

- script kiddies, lone hackers, hacktivists
- range of skills, TTPs and skills
- in it for the “lulz,” fame, maybe financial gain

Business Man:

- lone hacker
- range of skills, TTPs
- programmer, hacker-for-hire, botmaster



Business:

- Organized criminals, nation-states
- financial gain, espionage

owners

actors

soldiers

COMMON MOTIVES AGAINST SLTTs

Alleged Use of Excessive Force by LEO

Perceived Injustice

Alleged Animal Cruelty by LEO

Alleged Offensive Comments

Anti-Government

Opportunistic

Unknown



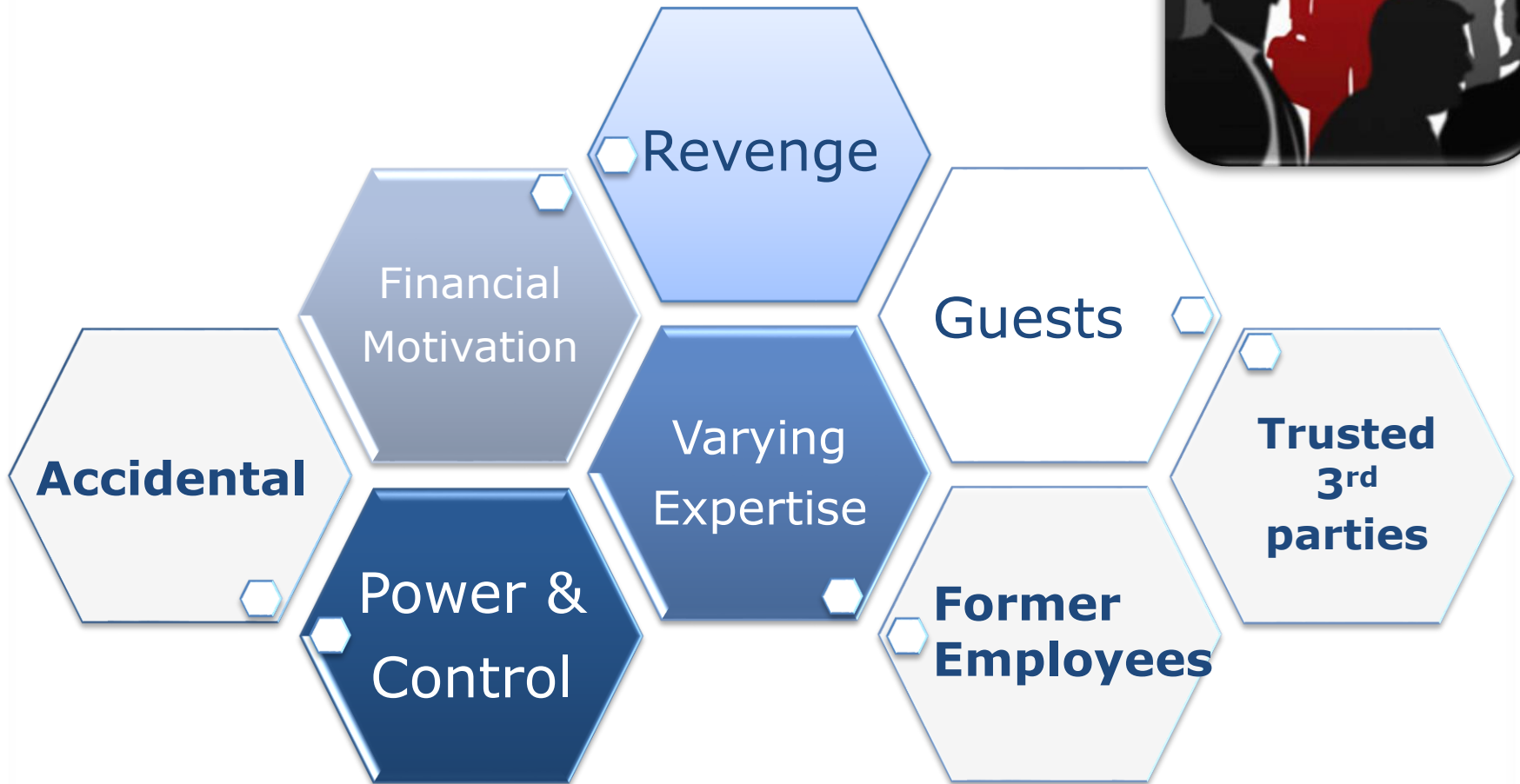
COMMON CTA TTPs



DDoS Attack
Doxing
Claimed SQLi
Website Defacement
Data Release
Claimed XSS
Compromised Computer/Server
Account Compromise
Spear Phishing
Phone Bomb
Scanning Activity



INSIDERS



EMPLOYEE MISTAKES

SSID: marko

Password: w3Lc0m3!HERE



EVERYONE MAKES MISTAKES...



The trick is to learn from them!

MS-ISAC MEMBERSHIP



MULTI-STATE
Information Sharing
& Analysis Center™

24 x 7 SECURITY OPERATIONS CENTER

Central location to report any cybersecurity incident

- **Support:**
 - Network Monitoring Services
 - Research and Analysis
- **Analysis and Monitoring:**
 - Threats
 - Vulnerabilities
 - Attacks
- **Reporting:**
 - Cyber Alerts & Advisories
 - Web Defacements
 - Account Compromises
 - Hacktivist Notifications



To report an incident or
request assistance:
Phone: 1-866-787-4722
Email: soc@msisac.org

MONITORING OF IP RANGE & DOMAIN SPACE

IP Monitoring

- IPs connecting to malicious C&Cs
- Compromised IPs
- Indicators of compromise from the MS-ISAC network monitoring (Albert)
- Notifications from Spamhaus

Domain Monitoring

- Notifications on compromised user credentials, open source and third party information
- Vulnerability Management Program (VMP)

Send domains, IP ranges,
and contact info to:

soc@msisac.org

VULNERABILITY MANAGEMENT PROGRAM

What Data Are We Collecting?

- Server type and version (IIS, Apache, etc.)
- Web programming language and version (PHP, ASP, etc.)
- Content Management System and version (WordPress, Joomla, Drupal, etc.)

Email notifications are sent with 2 attachments containing information on out-of-date and up-to-date systems:

- Out-of-Date systems should be patched/updated and could potentially have a vulnerability associated with it
- Up-to-Date systems have the most current patches

SOLTRA EDGE

Machine-to-Machine indicator transfer



To gain an account
contact:
VMP@cisecurity.org

MALICIOUS CODE ANALYSIS PLATFORM

A web based service that enables members to submit and analyze suspicious files in a controlled and non-public fashion

- Executables
- DLLs
- Documents
- Quarantine files
- Archives

To gain an account contact:
soc@msisac.org



COMPUTER EMERGENCY RESPONSE TEAM (CERT)


- Incident Response (includes on-site assistance)
- Network & Web Application Vulnerability Assessments
- Malware Analysis
- Computer & Network Forensics
- Log Analysis
- Statistical Data Analysis
- Penetration Testing

To report an incident or
request assistance:

Phone: 1-866-787-4722

Email: soc@msisac.org

MS-ISAC ADVISORIES

 This message was sent with High importance.

From: MS-ISAC Advisory

Sent: Thu 10/15/2015 10:19 AM

To: Thomas Duffy

Cc:

Subject: MS-ISAC CYBER SECURITY ADVISORY - Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution (APSB15-25) - TLP: WHITE

TLP: WHITE
MS-ISAC CYBER SECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2015-119 - UPDATED

DATE(S) ISSUED:
10/13/2015
10/15/2015 - Updated

SUBJECT:
Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution (APSB15-25)

OVERVIEW:

Multiple vulnerabilities in Adobe Flash Player could allow remote code execution. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, compromising processing resources in a user's computer, or remote code execution. Failed exploit attempts will likely cause denial-of-service conditions.

THREAT INTELLIGENCE

There are currently no reports of these vulnerabilities being exploited in the wild.

October 15 – UPDATED THREAT INTELLIGENCE

Adobe is aware of a report that an exploit for the CVE-2015-7645 critical vulnerability is being used in limited, targeted attacks.



MONTHLY NEWSLETTER

Distributed in template form to allow for re-branding and redistribution by your agency

March 2016
Volume 11, Issue 3

Why Strong, Unique Passwords Matter



MULTI-STATE
Information Sharing
& Analysis Center™

Monthly Security Tips
Newsletter

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

Cybersecurity experts continually identify the use of *strong, unique* passwords as one of their top recommendations. However, this is also one of the least commonly followed recommendations because unless you know the tricks, it's difficult to remember *strong, unique* passwords for every login and website.

Why Strong, Unique Passwords Matter

Cybersecurity experts make the recommendation for *strong, unique* passwords for several reasons – the first being that every day malicious cyber threat actors compromise websites and online accounts, and post lists of usernames, email addresses, and passwords online. This exposes people's passwords, and worse yet, they are exposed with information that uniquely

A strong password consists of at least 10, and includes a combination of uppercase and lowercase letters, numbers, and symbols. A unique password is a password that is only used with one account.

NATIONAL WEBCASTS


a collaborative effort between DHS and MS-ISAC
to provide timely and relevant cybersecurity
education and information

- Prioritize Your NIST CSF Implementation with the CIS Critical Security Controls (June)
- Internet of Things (April)
- 2016 Predictions from the MS-ISAC (February)
- Cybersecurity Year in Review and 2016 Preview (December 2015)
- National Cybersecurity Awareness Month: Tips for Staying Safe Online (October 2015)

<https://msisac.cisecurity.org/webcast/>

WEEKLY MALWARE IPs AND DOMAINS

From: MS-ISAC SOC
To: MS-ISAC SOC
Cc:
Subject: Message from the MS-ISAC: Malware IPs and Domains observed by MS-ISAC 11/23/2015 - 11/29/2015 - TLP: GREEN
Sent: Mon 11/30/2015

Message  IPs of Interest 11-23 to 11-29.xlsx (35 KB)

Attached to this email is a list of IP addresses and domains associated with malware observed by MS-ISAC from 11/23/2015 - 11/29/2015 using the network security services.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

This list is produced from data collected by the MS-ISAC. Currently this data is being collected across a number of States and Local Governments.

The spreadsheet contains four tabs with the following information:

1. Malware IP Data

IP Address – This is either the IP address that is attacking a system or the IP address malware on an infected system is communicating with.

Counts – This is the number of alerts generated for malicious traffic to or from the IP address.

Country, Region, City – Location of the potentially malicious IP address.

ISP/Host – ISP or Hosting provider for the IP address.

Comment – Malware type or activity associated with the infection.



MS-ISAC CYBER ALERTS

MS-ISAC Advisory

Sent: Thursday, June 16, 2016 at 2:57 PM

To: Thomas Duffy

TLP: WHITE MS-ISAC CYBER ALERT

TO: All MS-ISAC Members, Fusion Centers, and IIC partners

DATE ISSUED: June 16, 2016

SUBJECT: Malicious Email Campaign Targeting Attorneys Spoofs Emails From Statewide Legal Organizations - TLP: WHITE

In June 2016 MS-ISAC became aware of a malicious email campaign targeting attorneys, which spoofs emails from statewide legal organizations, such as the Bar Association and the Board of Bar Examiners. The subject and body of the emails include claims that “a complaint was filed against your law practice” or that “records indicate your membership dues are past due.” Recipients are asked to respond to the claims by clicking a link which leads to a malicious download, potentially ransomware.

The emails are well written and appear to originate from the appropriate authority, such as an Association official, likely increasing their effectiveness. Reporting from various states indicates a likelihood that this campaign is personalized to individuals practicing in a particular state and may be progressing on a state-by-state basis. The following states have been referenced in public reporting on this campaign: Alabama, California, Florida, Georgia, and Nevada. This targeting may include attorneys working for state, local, tribal, and territorial (SLTT) governments.

Recommendations:

MS-ISAC recommends the following actions:

- Share this information with potentially impacted organizations your area of responsibility, including Departments of Law/Justice, related law enforcement agencies, and agency-specific offices of counsel.
- Train government legal professionals in identifying spear phishing emails which may include spoofed email addresses, unusual requests, and questionable and/or masked links. This particular series of emails includes what appears to be a link to the state bar association, but when the user hovers over the link it shows that the link is really to a different website. Copying and pasting the link, instead of clicking on it, would defeat this social engineering attempt.
- Perform regular backups of all systems to limit the impact of data loss from ransomware infections. Backups should be stored offline.



MS-ISAC INTEL PAPERS

UNCLASSIFIED//FOR OFFICIAL USE ONLY • Traffic Light Protocol: GREEN

**Multi State Information Sharing and Analysis Center
Cyber Monthly Update**

Information current as of May 31, 2016



Federal Awareness

(U) TLP: **WHITE** The Center (NCCIC)/Industrial Review report highlights capabilities in the 16 countries and their coordination efforts in operations and upgrading the number of incident response reported vulnerabilities, as available at: <https://ics-cs.com> Year in Review FY2015 F

Insert your logo here

Traffic Light Protocol: WHITE



MULTI-STATE
Information Sharing
& Analysis Center™

MS-ISAC Security Primer
Spear Phishing
SP2016-0518

Spear Philanthropy
March 23, 2016, SP2016-0518

TLP: WHITE Overview: Cyber threat actors utilize phishing emails to compromise systems, networks, and/or gather information using social engineering techniques. A phishing email is designed to prompt a response from the recipient, such as clicking on a link or opening an attachment. Through the response, the recipient may download malware or be redirected to a website prompting them to provide sensitive information, such as login credentials, that will be sent to the cyber threat actors. Spear phishing involves a cyber threat actor sending targeted emails to a small group of users.

Other types of phishing include:

- Smishing ("SMS phishing") involves a user opening a malicious SMS, or text, message on a mobile device.
- Vishing involves a cyber threat actor attempting to gather information over Voice over IP (VoIP) phones.
- Whaling is a spear phishing attempt directed towards a senior executive or other high profile target.



MULTI-STATE
Information Sharing
& Analysis Center™

DESK REFERENCE

Quarterly Identified Cyber Threat Actor Review

Information from October 1 to December 31, 2015

(U) TLP: **AMBER** This desk reference provides a review of the most active, identified¹ Cyber Threat Actors^{2,3} (CTA) and malicious cyber campaigns and operations from October 1 through December 31, 2015. The information in this document is provided to further the reader's

Traffic Light Protocol: WHITE



MULTI-STATE
Information Sharing
& Analysis Center™

**TECHNICAL
WHITE PAPER**
February 2016

2016

Timely Patching Reduces System Compromises
 February 2016
 Authored by: Katelyn Bailey, Cyber Intel Analyst

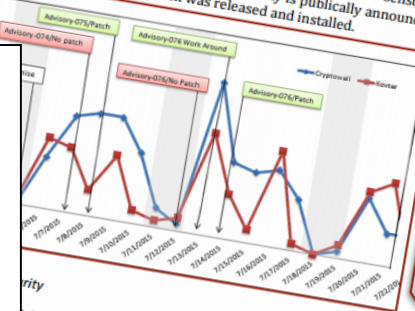
Training Reduces System Compromise

Updates System Compromises

updates address software vulnerabilities that may allow malicious cyber to information systems or a network. Once vulnerabilities are publicly information is available to anyone, actors. It is essential to quickly as the disclosed information threat actors to exploit.

The primary infection vector in at least 95% of all the incidents investigated by MS-ISAC was an unpatched vulnerability in an operating system, software, or plugin.

exploits that targeted vulnerabilities in common software. The Angler botnet, the CryptoWall and Kovter malware in July 2015, incorporated the dates of patch releases to the public. The below graph shows the number of infections detected by MS-ISAC sensors and the attempted CryptoWall patch releases. After the vulnerability is publicly announced, a sharp decrease in the number of infections is observed.



MS-ISAC recommends implementing a routine patching program and applying critical patches immediately after appropriate testing.

Traffic Light Protocol: WHITE
be distributed without

Traffic Light Protocol: WHITE
information may be distributed without restriction, subject to copyright controls.

1



MULTI-STATE
Information Sharing
& Analysis Center™

MS-ISAC Membership

FEE BASED SERVICES

- Network Monitoring (Albert)
- Managed Security Services (MSS)
- Web application vulnerability assessments
- Network vulnerability assessments
- Penetration testing
- Phishing engagements
- Security assessments

For more info on any of these contact:
info@msisac.org

MS-ISAC ANNUAL MEETING



**2016
Location...**

**San Antonio,
TX!**



WHAT CAN YOU DO?

Low Hanging Fruit!

1. PATCH!
2. Use defensive software
3. Back-up
4. Train users
5. Enforce strong, complex, unique passwords



Critical Security Controls

1. Identify authorized and unauthorized devices
2. Inventory authorized and unauthorized software
3. Secure configurations for hardware and software
4. Continuous vulnerability assessment and remediation
5. Controlled use of admin privileges

IDENTIFY MALICIOUS ACTIVITY

- Antivirus
- Firewalls
- IDS/IPS
- Logs (90 days!)
- Places to Look
 - Pastebin, Ghostbin, Zerobin
 - Twitter
 - Facebook
 - Google
 - SHODAN
- Things to Look For:
 - Announcements
 - Hashtags
 - Doxings



Hacktivist DDoS Claim

SHARE INFORMATION

- **Be prepared**
 - Learn from others' best practices
 - Gather intel to help you be proactive
- **Be willing to ask for help**
 - Identify other resources to augment what you are doing
- **Be a part of the solution**
 - Take part in information sharing

WHO DO I CALL?

Security Operations Center (SOC)

SOC@cisecurity.org - 1-866-787-4722

31 Tech Valley Dr., East Greenbush, NY 12061-4134

www.cisecurity.org



**to join or get more information:
[https://msisac.cisecurity.org/memb
ers/index.cfm](https://msisac.cisecurity.org/members/index.cfm)**

MS-ISAC CONTACT NUMBERS

Thank You!

Erin Dayton
Erin.Dayton@Cisecurity.org

Security Operations Center

24/7 Phone Number

1-866-787-4722

soc@msisac.org

MS-ISAC HQ

Front Desk

518-266-3460

info@msisac.org